UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/461,010	12/15/1999	PIERRE CALVEZ	6313	3226

7590 06/15/2005

EDWARD J KONDRACKI
MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 221023833

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/461,010	CALVEZ ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-54* is/are pending in the application.

4a) ~~Of the above~~ claim(s) *1-19* is/are ~~withdrawn from consideration.~~ cancelled

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 April 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/19/2005 has been entered.

Claims 1-19 were cancelled previously. Claims 20, 29, 47, and 51-52 were amended. Claims 20-52 are pending. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Amendment

The amendment filed 5/19/2005 amended independent claims 20, 29, 47, and 51-52 with a limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done." The examiner asserts that this limitation is obvious and known in the art as the recited attributes are often used to describe various objects or

processes for the purpose of status indication. The examiner will also cite art below for a rejection of this limitation. The examiner notes that applicant did not make any arguments or amendments to the dependent claims, so the examiner assumes that applicant agrees that the former examiner's rejection of the dependent claims were proper. The examiner also notes that no arguments were raised by the applicant regarding the rejection of the independent claims prior to applicant's current amendments to the independent claims. As such, the examiner assumes applicant agrees with the former examiner's rejection of those limitations that were present before applicant amended the independent claims. The examiner will copy and paste the appropriate rejection of limitations of the previous examiner into this action as necessary for purposes of record keeping and clarity.

Drawings

The drawings are objected to because in Fig 1, item 9 is indicated in the drawing as a "wake up mechanism." In the specification, item 9 is called a key server (see p6, line 3). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for

consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The last sentence of the abstract contains the legal phraseology "said process."

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 20-54 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Independent claims 20, 29, 47, and 51-52 all recite a similar limitation which states "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certificate request and done." The examiner respectfully submits that the some of the values stated above conflict with each other in nature, therefore the use of "and" in the series renders the claims indefinite. For example, something cannot be both "in progress" and "done" at the same time. The examiner believes applicant may have meant to recite, "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certificate request, **or** done."

Also, for the same limitation recited above for the independent claims, the examiner notes that the limitation seems to be supported in the specification on p9, lines 24-26 and on p10, lines 26-28. However, the specification does not specifically have a limitation wherein the attribute value is "sending a certificate request." The closest support for this limitation in the specification seems to be "sending a creation request." The examiner respectfully submits that the limitation of "sending a certificate request" is much broader than "sending a creation request" and in the course of examining this application, the examiner will give the claim language the broadest, reasonable interpretation to "sending a certificate request."

Any claims not specifically addressed are rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 47, 48, 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Andrews et al (US 6,324,645).

Claim 47:

With respect to Claim 47 the limitation "a computer system for creating and managing pairs of asymmetrical cryptographic keys and certificates associated with the pairs of keys, the pairs of keys and the certificates being intended for subjects managed by said system, comprising a key generating center for creating at least one pair of keys at the request of a local registration authority with which the key generating center communicates; at least one certification authority to which the system has access for creating a certificate at the request of the local registration authority and means for automating, based on one or more attributes associated with one or more subjects, the creation and/or certification of at least one pair of keys for each subject managed by the system" is met by Ishii on column 5, lines 44-67, column 8, lines 8-24 and Fig. 2. In the cited reference, there exists a secret key (private key) generation unit, a public key generation unit and a certification production unit. The tamper resistant personal device represents the local registration authority. It is in communication with the key-generating center. The key-generating center is both the secret/private and public generating center (see Fig. 2). After the user's personal

information is entered, the personal device communicates with the other modules within to generate the key pairs and certificate.

Hence, it would have been obvious to have the tamper resistant personal device as the local registration authority because the personal portable device is in communication with the key generating center(s) and requests the creation of a key pair, after the user enters his/her personal information (see Ishii, Fig. 4 and column 7, lines 64-67, column 8, lines 1-3). Furthermore it is obvious that the process of creating and/or certificate of at least one pair of keys is automated because Figure 4 clearly shows that after the user enters his/her personal information, the key pair and certificate is generated without any user intervention. Hence, the process is automated.

The above was from the previous office action. The examiner will now address the new limitation as amended by the applicant on 5/19/2005. Ishii does not explicitly disclose the limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done."

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. The certificate itself can be considered a subject. Therefore, at the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art, in light of Andrews's teachings, to have modified Ishii's invention according to the limitation recited in claim 47. One of ordinary skill would have been motivated to

incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Claim 48:

With respect to Claim 48, the limitation "a central management service for creating, updating and consulting objects and subjects managed by said system a local registration authority for handling the creation and/or the certification of keys intended for the objects and the subjects a central security base containing the subjects and the objects managed by the system with which the local registration authority communicates a key generating center for creating at least one pair of keys at the request of the local registration authority with which the key generating center communicates; and at least one certification authority to which the system has access for creating a certificate at the request of the local registration authority" is met by Ishii on Figure 5.

Claim 52:

With respect to Claim 52, the limitation "a computer system for creating symmetrical cryptographic keys, wherein a symmetrical cryptographic key can be used to both encode and decode data" is met by Ishii on column 1, lines 26-29; and wherein said system manages subjects, characterized in that it comprises a key generating center for creating at least one pair of keys at the request of the local registration authority with which the key generating center communicates; at least one certification authority to which the system has access for creating a certificate at the request of the

local registration authority and means for automating, based on one or more attributes associated with one or more subjects, the creation of at least one key for each subject managed by the system" is met by Ishii on column 11, lines 50-67 and column 12, lines 1-46.

The above was from the previous office action. The examiner will now address the new limitation as amended by the applicant on 5/19/2005. Ishii does not explicitly disclose the limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done."

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. The certificate itself can be considered a subject. Therefore, at the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art, in light of Andrews's teachings, to have modified Ishii's invention according to the limitation recited in claim 52. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Claims 49 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Andrews et al (US 6,324,645) and further in view of Van Oorschot (US 6,370,249).

Claims 49 and 50:

With respect to Claims 49 and 50, all the limitations are met by Ishii and Andrews except the limitation below.

The limitation of "a wake up mechanism periodically waking up the local registration authority" is met implicitly by Van Oorschot on column 3, lines 14-19. The time-to-time provision of a public key to a client implicitly discloses that the system would need to be alert from at these frequent time intervals and hence this necessitates a wake up mechanism.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination system of Ishii and Andrews because a wake up mechanism is necessary for continuous generation and replacement of old keys and certificates, hence yielding a more current, more secure key generation system.

Claims 20, 21, 29, 30, 33, 45, 46, 51, 53, 54, 55, 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith (US 6,651,166) and further in view of Andrews et al (US 6,324,645).

Claim 20:

With regards to Claim 20, the limitation "creating, based on the one or more attributes, at least one first individual creation and certification request for a pair of asymmetric keys for said subject" is met by Ishii on column 11, lines 20-33 and 63-67.

The limitation "transmitting a key generation request corresponding to said first individual creation and certification request to a key generating center (8), which issues a pair of asymmetric keys in accordance with said key generation request" is met by Ishii on column 11, lines 20-62.

The limitation "creating at least one second individual certification request the public key created for said subject" is met by Ishii on column 11, lines 20-33, 63-67.

The limitation "transmitting a certification authority request corresponding to said second individual certification request to a certification authority, and issuing a first certificate in accordance with said certification authority request" is met by Ishii on column 12 on lines 12-16, 42-46. Further, the limitation of "creating a public key for said subject" is met by Ishii on column 11, lines 60-62. Ishii however does not disclose searching a storage means for the subject that needs the asymmetric keys. This is however disclosed by Smith.

The limitation "searching in storage means for one or more attributes, the attributes specifying one or more subjects for which a pair of asymmetric keys and an associated certificate must be created" is met by Smith et al on column 5, lines 24-35. In Smith, the client information is stored and retrieved (when being compared); afterwards the key pair is generated.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii because retrieval of the subject's data from storage is a necessary step towards creation of a pair of keys and a corresponding certificate.

The above was from the previous office action. The examiner will now address the new limitation as amended by the applicant on 5/19/2005. Ishii and Smith do not explicitly disclose the limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done."

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. The certificate itself can be considered a subject. Therefore, at the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art, in light of Andrews's teachings, to have further modified Ishii and Smith's combination invention according to the limitation recited in claim 20. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Claim 21:

With respect to Claim 21, the limitation of "creating the pair of keys for a given subject when said subject lacks the pair of keys and the corresponding first individual creation and certification request" is met by Ishii in column 4, lines 16-36; column 28, lines 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20.

Claim 29:

With respect to Claim 29, the limitation "creating at least one individual certification request for certifying a public key" is met by Ishii on column 11, lines 63-67.

The limitation "transmitting a certification authority request corresponding to said individual certification request to a certification authority, and issuing a certificate in accordance with said certification authority request" is met by Ishii on column 12, lines 12-16 and 42-45; and "creating, based on the one or more attributes, at least one individual certification request for certifying a public key" is met by Ishii on column 11, lines 20-33, 63-67. Ishii however does not disclose searching the storage means for a pair of asymmetric keys. This is disclosed by Smith.

The limitation "searching in storage means for one or more attributes, the attributes associated with one or more subjects for which a certificate must be created" is met by Smith et al on column 5, lines 24-35 and 38-52.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii because referring back to an already secure storage means for the necessary keys allows the system to save the time it would have used to request and authenticate the sender of the keys from a remote area.

The above was from the previous office action. The examiner will now address the new limitation as amended by the applicant on 5/19/2005. Ishii and Smith do not explicitly disclose the limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done."

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. The certificate itself can be considered a subject. Therefore, at the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art, in light of Andrews's teachings, to have further modified Ishii and Smith's combination invention according to the limitation recited in claim 29. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Claim 30:

With respect to Claim 30, the limitation "certificate for a given subject when said subject lacks the certificate and the individual certification request" is met by Ishii on column 28, lines 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20.

Claim 33:

With respect to Claims 33, the limitation "creating the certificate for a given subject when the certificate expires" is met by Ishii on column 12, lines 17-50.

Claim 45:

With respect to Claim 45, the limitation "comprising performing the encoding of one or more extensions in accordance with one or more given rules and of entering the encoded extension or extensions into the individual certification request during the creation of said individual certification request" is met by Ishii on column 11, lines 63-67 and column 12, lines 1-3.

Claim 46:

With respect to Claim 46, the limitation "changing the value of the attribute contained in each of the individual first and second requests to indicate status of the process" is met by Ishii on Fig. 20 and 21.

Claim 51:

With respect to Claim 51, the limitation "creating, based on the one or more attributes, at least one individual request for creating a symmetric key for said subject" is met by Ishii on column 1, lines 26-29, column 11, lines 20-21 and 31-33. A secret key cryptosystem is the same thing as a symmetrical cryptosystem because of the use of the same key to encrypt and decrypt. These symmetrical keys, as disclosed on column 1 are much faster than their asymmetrical counterparts. Hence for the advantage of increasing processing speed, they can intuitively be substituted for the asymmetrical keys in the invention disclosed on column 11.

The limitation "transmitting a key generating request corresponding to said individual creation request to a key generating center (8)" is met by Ishii on column 11, lines 31-33.

The limitation "issuing by said key generating center a symmetric key in accordance with said transmitted key generating request" is met by Ishii on column 11, lines 35-62. Ishii however does not disclose a storage means as disclosed below. The limitation "searching in storage means for one or more attributes, the attributes specifying one or more subjects for which a symmetric key must be created" is partly met by Smith et al on column 5, lines 24-35. In Smith et al, this input information is retrieved from the SDCE server before the key pair is generated.
It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii as to achieve high speed processing.

The above was from the previous office action. The examiner will now address the new limitation as amended by the applicant on 5/19/2005. Ishii and Smith do not explicitly disclose the limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done."

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. The certificate itself can be considered a subject. Therefore, at the time the

applicant's invention was made, it would have been obvious to one of ordinary skill in the art, in light of Andrews's teachings, to have further modified Ishii and Smith's combination invention according to the limitation recited in claim 51. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Claims 53 and 54:

With respect to Claim 53 and 54, the limitation of "creating a pair of keys for a given subject when a certificate issued in response to a certification authority request for a pair of keys for said subject intended for an identical use has been revoked and a new pair of keys been requested" is met by Ishii on column 28: 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20. Revocation will occur intuitively if the device/key(s) is lost/stolen/destroyed, hence the need to reissue/create a new set of keys. The secret key is reproduced first and the public key is reproduced shortly afterwards.

Claim 55:

Ishii does not disclose, "periodically activating a local registration authority to perform the searching step." However, this limitation is met by Smith et al on column 5, lines 28-31, 60-62.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within Ishii's modified

system because retrieval of the subject's data from storage is a necessary step towards creation of a pair of keys and a corresponding certificate.

Claim 56:

Ishii does not disclose, "wherein an activation period is modifiable." However, this limitation is obvious over by Smith et al on column 5, lines 28-31, 60-62.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within Ishii's modified system because retrieval of the subject's data from storage is a necessary step towards creation of a pair of keys and a corresponding certificate.

Claims 22, 31, 32, 34, 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith et al (US 6,651,166) and Andrews et al (US 6,324,645) in further view of Van Oorschot (US 6,370,249).

Claim 22:

With respect to Claim 22, the combination of Ishii, Smith, and Andrews meets all the limitation except that of periodical generation of keys and certificates.

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii, Smith, and Andrews because a periodical generation of new keys provides a more secure computer system.

Claims 31 and 32:

With respect to Claim 31 and 32, the combination of Ishii, Smith, and Andrews meets all the limitation except that of periodically executing the process.

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii, Smith, and Andrews because a periodical generation of new keys provides a more secure computer system.

Claims 34 and 35:

With respect to Claims 34, 35 the limitation "creating the new certificate for a given subject when the first certificate expires" is met by Ishii on column 12, lines 17-50.

Claims 23, 24, 25, 26, 27, 28, 36, 37, 38, 39, 40, 41, 42,43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith et al (US 6,651,166) and Andrews et al (US 6,324,645) in view of Van Oorschot (US 6,370,249) in further view of Aziz (US 6,330,671).

Claims 23-25:

With respect to Claim 23-25, the combination of Ishii, Smith, and Andrews meets all the limitation except that described below.

The limitation "wherein each individual first and second request is created from corresponding multiple creation and certification requests stored in the storage means..." is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii, Smith, and Andrews to allow for the secure creation of keys for the required authorized individual.

The combination of Ishii, Smith, Andrews and Van Oorschot however does not disclose a set of subjects belonging to a preset list. This is however disclosed by Aziz. The limitation "relative to a set of subjects belonging to a preset list or to a set of subjects defined by predetermined criteria, as well as to model pairs of keys and associated model certificates for the set in question" is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Aziz within the combination of Ishii, Smith, Andrews and Van Oorschot so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual.

Claims 26-28:

With respect to Claims 26-28, Ishii does not disclose "searching in each of the multiple creation and certification requests for all of the subjects in a condition such that

a pair of keys must be created." However, this limitation is met by Van Oorschot on column 4, lines 37-47.

It would have been obvious to one of ordinary skill in the art at the time the invention was in light of the above to have further modified the combination invention of Ishii, Smith, Andrews, Van Oorschot, and Aziz according to the limitations recited in claims 26-28. One of ordinary skill would have been motivated to do so as to find the correct and authorized recipient of the keys, and hence prevent the sending of keys to an unauthorized individual.

Claims 36-39:

With respect to Claim 36-39, Ishii does not disclose, "creating each individual request from a corresponding multiple certification request recorded in the storage means...." However, this limitation is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Van Oorschot to the combination of Ishii, Smith, and Andrews so as to allow for the secure creation of keys for the required authorized individual.

Ishii also does not disclose the set of keys belonging to a preset list of keys. This is however disclosed by Aziz.

The limitation "...relative to a set of pairs of keys for subjects belonging to a preset list or to a set of pairs of keys for subjects defined by predetermined criteria, as well as to associated model certificates for the set in question" is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Aziz within the combination of Ishii, Smith, Andrews, and Van Oorschot so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual.

Claims 40-43:

Ishii does not disclose "searching in each of the multiple creation and certification requests of the system for all of the subjects in a condition such that a pair of keys must be created." However, this limitation is met by Van Oorschot on column 4, lines 37-47. In light of this, it would have been obvious to one of ordinary skill in the art to further modify the combination of Ishii, Smith, Andrews, Van Oorschot, and Aziz so as to allow for the creation and distribution of secure keys.

Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith (US 6,651,166) and Andrews et al (US 6,324,645) in further view of Schneier.

With respect to Claim 44, the combination of Ishii, Smith, and Andrews meets all the limitation except for the limitation disclosed below.

The limitation "wherein each multiple request comprises an attribute relative to at least one execution date and in that said process comprising of including in the search

only the multiple requests whose expiration date has arrived" is met by Schneier on page 183-184, section 8.10.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Schneier within the combination of Ishii, Smith, and Andrews so as to prevent the existence of keys for an extended period of time and hence lessen the likelihood of the keys being compromised as disclosed by Schneier within the same citation.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KIM VU
SUPERVISORY PATENT EXAM
TECHNOLOGY CENTER 2